94

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,509	02/04/2002	Yoshihito Ishibashi	SONY JP-141	9631

530 7590 10/05/2005

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/937,509	**Applicant(s)** ISHIBASHI ET AL.
	Examiner Kaveh Abrishamkar	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *02/04/2002*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on February 4, 2002. Claims 1-53 were originally received for consideration. No preliminary amendments for the claims were received. Claims 1-53 are currently being considered.

Information Disclosure Statement

2. An initialed and dated copy of Applicant's IDS form 1449, received on February 4, 2002, is attached to this Office action.

Specification

3. The abstract of the disclosure is objected to because the abstract in an application filed under 35 U.S.C. 111 may not exceed 150 words in length. Correction is required. See MPEP § 608.01(b).

4. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

5. Claim 43 is objected to because of the following informalities: Claim 43 is number as claim 15, and in the first line it is said to depend on claim 43. This has been interpreted as being number as claim 43 and being dependent on claim 42 for purposes of examination. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

7. Regarding claim 4, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

8. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The first limitation states that setting information is stored, but does not designate what the setting information is, or what it is used for.

9. Claim 17 recites the limitation "said storing" in the first line of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1-53 are rejected under 35 U.S.C. 102(b) as being anticipated by Ishiguro et al. (U.S. Patent 5883,958).

Regarding claims 1, 13 20 and 28, Ishiguro discloses:

A data processing system comprising a recorder/reproducer and a recording device for executing transmission of encryption data to each other.

The recording device has a data storing section for storing content data (column 3 lines 14-22) that is transferable between the recorder/reproducer and the recording device, and at the same time, has a plurality of key blocks (column 3 lines 48-67) storing key data applicable at least to authentication processing between the recorder/reproducer and the recording device, and the key data stored in the plurality of key blocks has a configuration in which different key data is stored for each block (column 3 lines 66-67), wherein said recorder/reproducer has a configuration for, in the authentication processing between the recorder/reproducer and the recording device, designating one key block out of the plurality of key blocks held by said recording device (column 4 lines 4-50), and executing the authentication processing with said recording device based on the key data stored in the designated key block (column 4 lines 27-50), wherein a challenge is produced from the key.

Claim 2, 14, and 21 are rejected as applied above in rejecting claims 1,13, and 20 respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that an authentication key that is applicable at least to the authentication processing is included in each of the plurality of key blocks of said recording device, and the authentication key of each key block is configured as key data different from each other (column 3 lines 66-67), wherein different public keys are used depending on the manufacturer.

Claims 3 and 22 are rejected as applied above in rejecting claim 1 and 20, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized by having a configuration in which:

said recorder/reproducer holds setting information in which a key block to be applied to the authentication processing as a designated key block in a memory in the recorder/reproducer (column 3 lines 42-48); and

said recorder/reproducer designates one key block out of the plurality of key blocks held by said recording device based on the setting information held in the memory in the recorder/reproducer when the authentication processing between the recorder/reproducer (column 4 lines 4-50), and the recording device is performed, and executes the authentication processing (column 4 lines 27-50), wherein a challenge is produced from the key.

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Ishiguro discloses:

The data processing system, characterized by having a configuration in which the designated key block setting information of said recorder/reproducer is set to be different for each predetermined product unit such as a model of the recorder/reproducer, a version or a delivery destination (column 3 lines 42-47).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Ishiguro discloses:

The data processing system, characterized in that:

said recorder/reproducer has a configuration in which authentication processing key data required for the authentication processing with said recording device is stored in the memory in the recorder/reproducer (column 3 liens 53-67); and

authentication of the authentication processing key data stored in said memory in the recorder/reproducer is only established in the authentication processing using a key data in a block stored in a part of the plurality of key blocks in said recording device, and is not established in the authentication processing using a key data in other key blocks (column 3 lines 53-67).

Claims 6, and 23 are rejected as applied above in rejecting claims 1 and 20, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that: said recorder/reproducer stores a master key Mkake for recording device authentication key in the memory of the recorder/reproducer (column 3 lines 54-67); and

an authentication key Kake that is generated based on said master key Mkake for recording device authentication key is an authentication key whose authentication is only established in the authentication processing using key data in a designated block set in the recorder/reproducer, and is not established in the authentication processing using key data in other key blocks (column 3 lines 66-67).

Claim 7, 15, and 24 are rejected as applied above in rejecting claims 6,13, and 20, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that:

said recording device has a configuration in which a recording device identification information IDmem in said memory in the recording device (column 3 lines 23-28) and, at the same time, an authentication key Kake that is different for each key block is stored in each of said plurality of key blocks (column 3 lines 66-67); and said recorder/reproducer has a configuration for generating the authentication key Kake by encryption processing of said recording device identification information IDmem based on the master key Mkake for recording device authentication stored in the memory of the recorder/reproducer, and performing the authentication processing with the designated key block of said recording device using the generated authentication key Kake (column 4 lines 27-42).

Claims 8 and 16 are rejected as applied above in rejecting claims 1 and 13, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that each key block of said recording device includes recording device identifier information that is peculiar information of the recording device, an authentication key and a random number generation key to be used in the authentication processing with the recorder/reproducer, and a storing key to be used in encryption processing of storage data in said data storage section (column 4 lines 27-56).

Claims 9, 17 and 27 are rejected as applied above in rejecting claims 8 and 16, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that:

said storing key stored in each of the plurality of key blocks of said recording device is key data that is different for each key block and, at the same time, is a key to be used in encryption processing with respect to stored data of said data storage section (column 9 lines 53-62); and

said recording device has a configuration for executing key exchange processing of the storing key in the recording device, and outputting encryption data by a key different from the storing key to outside the recording device if utilization request of data that is encrypted by the storing key received from outside the recording device (column 9 lines 53-62).

Claims 10, 18 and 25 are rejected as applied above in rejecting claims 1, 13, and 20, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that:

said recording device has an encryption processing section (column 9 lines 50-67); and

the encryption processing section has a configuration for selecting one key block of the plurality of key blocks of the recording device in accordance with the key block designation information received from said recorder/reproducer, and executing the authentication processing with said recorder/reproducer using the key data in the selected key block (column 4 lines 4-50).

Claims 11, 19 and 26 are rejected as applied above in rejecting claim 10, 18, and 20. Furthermore, Ishiguro discloses:

The data processing system, characterized in that the encryption processing section of said recording device has a configuration for executing the encryption processing executed in the data storing processing in the data storing section storing content data transferable between the recorder/reproducer and the recording device and in the data transfer processing from the data storing section, using the key data in one key block that is selected in accordance with the key block designation information received from said recorder/reproducer (column 9 lines 53-67).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Ishiguro discloses:

The data processing system according to claim 1, characterized in that there are a plurality of designatable key blocks in said recording device in said recorder/reproducer, and at least one key block in the plurality of designatable key blocks is configured as a commonly designatable key block that is also designatable in other recorder/reproducers (column 3 lines 48-67).

Regarding claims 29,38,46 and 53, Ishiguro discloses:

A data processing system comprising a first apparatus and a second apparatus for executing transmission of encryption data to each other, characterized in that:
said second apparatus has an encryption processing section for executing encryption processing for transmission data with said first apparatus (column 9 lines 53-67);

said encryption processing section has a control section for receiving a command identifier transferred from said first apparatus in accordance with a setting sequence defined in advance, taking out a command corresponding to the received command identifier from a register, and having the command executed (column 3 lines 23-65, column 4 lines 6-15), wherein the identification is sent, and if the identification (command identifier) matches the entry in the key table (setting sequence) the authentication (command) is executed; and

the control section has a configuration for, if the command identifier transferred from the first apparatus is a command identifier different from the setting sequence, canceling processing of command corresponding to the command identifier (column 4 lines 16-23).

Claims 30, 39 and 47 are rejected as applied above in rejecting claims 29, 38, and 46, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized by having a configuration in which:

the setting sequence relating to the command identifier received from the first apparatus held by the control section is a command number setting sequence in which numbers are sequentially incremented (column 4 lines 16-23); and

said control section stores a received value of the command number received from said first apparatus in a memory, determines coincidence of a new command number received from said first apparatus with the setting sequence based on the received command number stored in said memory and, if it is determined that the new received command number is different from the setting sequence, executes resetting of the command number stored in said memory without performing command processing corresponding to the new received command number (column 4 lines 16-23), wherein if the identifier does not match the entry in the key table, the flag is reset to zero.

Claims 31,40, and 48 are rejected as applied above in rejecting claims 29, 38, and 46, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that:

said second apparatus has a command register storing a command in accordance with said setting sequence (column 4 lines 6-23), wherein the key table stores keys corresponding to received IDs (commands) and performs authentication using the key (column 3 lines 53-67);

an authentication processing command sequence for executing authentication processing between said first apparatus and said second apparatus, and an encryption processing command sequence for executing encryption processing relating to transferred data between said first apparatus and said second apparatus (column 3 lines 23-65, column 4 lines 6-15), wherein the identification is sent, and if the identification (command identifier) matches the entry in the key table (setting sequence) the authentication (command) is executed; and

a sequence is set such that a command identifier corresponding to said authentication processing command sequence is executed in a step before a command sequence corresponding to said encryption processing command sequence (column 4 lines 27-56), wherein authentication is performed before a session key is used to encrypt the data.

Claims 32, 41, and 49 are rejected as applied above in rejecting claims 31, 40, and 48, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that said encryption processing command sequence includes at least one of a command sequence including encryption key exchange processing for encryption data that is transferred from said first apparatus to said second apparatus and stored in storing means in said second apparatus, or a command sequence including an encryption key exchange processing for encryption data that is stored in the storing means in said second apparatus and transferred from said second apparatus to said first apparatus (column 3 lines 23-65, column 4 lines 6-15).

Claims 33, 42, and 50-51 are rejected as applied above in rejecting claims 31,40, and 48, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that said control section set an authentication flag indicating that authentication is done if authentication is established by the authentication processing of said first apparatus and said second apparatus, and executes command management control that enables execution of said encryption processing command sequence during the authentication flag is set, and said control section resets said authentication flag in executing said authentication processing command sequence anew (column 3 line 49 - column 4 line 27), wherein a validation (authentication) flag is set if the key is valid corresponding to the ID.

Claims 34, 43, and 52 are rejected as applied above in rejecting claims 32, 42, and 49, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized in that said data processing system has a configuration in which said control section manages an order of command execution based on said setting sequence and said command identifier in said encryption key exchange processing (column 4 lines 6-57), wherein authentication is performed before the encryption processing, and

said control section does not accept command processing that is different from said setting sequence from an external apparatus including said first apparatus during a series of command execution relating to said key exchange processing column 3 line 49 - column 4 line 27), wherein a validation (authentication) flag is set if the key is valid corresponding to the ID, and ifs not valid, authentication is not performed.

Claim 35 is rejected as applied above in rejecting claim 29. Furthermore, Ishiguro discloses:

The data processing system, characterized in that:

said second apparatus is a storage device having a data storage section for storing encryption data (Figure 1 item 2);

said first apparatus is a recorder/reproducer for performing storing processing of data in said storage device, and taking out data stored in said storage device to reproduce and execute the data (Figure 1 item 11); and

said recorder/reproducer has an encryption processing section for executing encryption processing of transferred data with said recording device (Figure 1 item 22).

Claims 36 and 44 are rejected as applied above in rejecting claims 35, and 38, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized by having a configuration in which:

said recording device has a key block storing an authentication key applied to authentication processing between said recorder/reproducer and said recording device and a storing key as an encryption key of data stored in a data storage section in said recording device (column 3 lines 48-67); and

said control section in an encryption processing section of said recording device receives a command identifier from said recorder/reproducer and executes authentication processing using the authentication key stored in said key block in accordance with said setting sequence (column 4 lines 4-50), and executes encryption processing of data accompanying key exchange processing using said storing key after completing the authentication processing (column 4 lines 27-42).

Claims 37 and 45 are rejected as applied above in rejecting claims 36 and 45, respectively. Furthermore, Ishiguro discloses:

The data processing system, characterized by having a configuration in which:

said key block is composed of a plurality of key blocks storing an authentication key and a storing key that are different each other (column 3 lines 48-67); and

said recorder/reproducer notifies said recording device of one key block used in authentication processing and encryption processing of data as a designated key block out of said plurality of key blocks (column 4 lines 4-50), and said recording device executes authentication processing using the authentication key stored in the designated key block (column 4 lines 4-50) and encryption processing of data using the storing key (column 4 lines 27-42).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3796. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

KA
09/30/2005